



American Hospital
Association®

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

June 3, 2019

Don Rucker, M.D.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C St SW, Floor 7
Washington, DC 20201

Re: RIN 0955-AA01, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program; Proposed Rule (Vol. 843, No. 42), March 4, 2019.

Dear Dr. Rucker:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to comment on the Office of the National Coordinator (ONC) for Health Information Technology's (IT) proposed rule on interoperability, information blocking and the ONC Health IT Certification Program. We appreciate your extension of the comment period given the rule's complexity and interaction with the Trusted Exchange Framework and Common Agreement proposals.

The AHA applauds ONC for addressing the critical issue of interoperability. We support a number of the proposed rule's provisions, including the exchange of patient data and the agency's focus on ensuring certified health IT products can provide core interoperability capabilities. When patients have access to their health information they can engage more fully in their care and experience better outcomes.

Our members strongly support patients having easy access to their health information so that they can be partners in their care. **However, we do not believe that patients should have to sacrifice data protections and data privacy in order to receive easy access to their health information.** We are deeply concerned that third party applications and tools not governed by HIPAA are increasingly accessing patient data and using it in ways in which patients likely are unaware. Patients' data is their own, and no organization, whether regulated by HIPAA or not, should be allowed to capitalize and



monetize their data without the patient fully understanding what is occurring and agreeing to it. **We urge ONC to consider the ramifications of its proposals and consider ways that we can help patients get easy access to their data without sacrificing their control or the protections HIPAA offers.**

In addition, we are opposed to the agency's interpretation of what may be included in the definition of electronic health information, specifically regarding price information. It goes well beyond what Congress intended and would seriously harm patients, hospitals and other health care providers.

While we appreciate the information blocking exception structure ONC has proposed, we are concerned that the burden of proof placed on hospitals and health systems to demonstrate that they did not information block when they, and their business associates, are trying to ensure that they are using and disclosing information only as they are legally permitted to do is much too great, and much too vague. ONC has a responsibility to provide significantly more detailed direction to hospitals and health systems and other HIPAA-covered entities about what documentation will be sufficient to demonstrate they did not engage in information blocking while they ensure that they remain in compliance with existing legal and regulatory obligations imposed by HIPAA and other laws.

Moreover, the agency has proposed to make the information blocking provisions effective the day the rule is finalized. This is impractical and leaves organizations no time to ensure they are in compliance, placing them in an inappropriately vulnerable position, for which noncompliance would have serious consequences.

We appreciate your consideration of these issues. Our detailed comments are attached. Please contact me if you have questions or feel free to have a member of your team contact Joanna Hiatt Kim, vice president of payment policy, at (202) 626-2340 or jkim@aha.org.

Sincerely,

/s/

Thomas P. Nickels
Executive Vice President

Enclosure

PRICE TRANSPARENCY

The AHA has several significant concerns about a number of the ideas floated in the proposed rule especially as it relates to the definition of electronic health information (EHI) and the disclosure of certain financial data that could adversely impact patients.

INCLUSION OF PRICE INFORMATION IN THE DEFINITION OF EHI

The AHA supports access to and the exchange and use of EHI, along with the prevention of information blocking. While access to EHI is an important goal, it is just as important to define EHI properly to reflect the intent of Congress and protect the legal rights and expectations of those affected by ONC's rules. The AHA believes that ONC's interpretation of what may be included in the definition of EHI goes well beyond what Congress intended and would cause serious harm. **Specifically, the AHA believes that ONC lacks authority to include price information – a term it leaves undefined – in the definition of EHI for purposes of determining what constitutes information blocking.**

Interpreting the definition of EHI to include price information would have serious untoward – even perverse – consequences. It likely would disrupt the health care system in many anticipated and unanticipated ways. The Federal Trade Commission (FTC) has warned against “broad disclosures of bids, prices, costs, and other sensitive information” noting “disclosing the terms of these health plan contracts might offer little incremental benefit to consumers, but could pose a substantial risk of reducing competition in health care markets.”¹ Furthermore, hospitals and other providers consider price information confidential. Allowing health plans to have access to that information could seriously disrupt negotiations with plans.

The AHA is particularly troubled by the way in which ONC apparently would require the disclosure of price information: It is an end-run around both the controlling statute and Administrative Procedure Act (APA). If Congress had intended to allow ONC to require hospitals to disclose price information to avoid being sanctioned for information blocking, it would have said so. It did not.

ONC is not permitted to circumvent congressional intent and the language of the statute. Unless and until Congress acts, we urge ONC not to interpret the definition of EHI to include price information or undertake “subsequent rulemaking to expand access to price information” as it has suggested it may do.

ONC Lacks Authority to Require the Disclosure of Price Information. We believe that Congress did not authorize ONC to require that price information be disclosed by

¹ Price Transparency or TMI? July 2, 2015, Tara Isa Koslov and Elizabeth Jex, Office of Policy Planning, Federal Trade Commission Blog. <https://www.ftc.gov/news-events/blogs/competition-matters/2015/07/price-transparency-or-tmi> (Price Transparency or TMI?).

hospitals. And the circuitous route ONC takes in explaining how it might mandate that hospitals disclose price information strongly suggests that ONC similarly recognizes the limits of its authority.

The provision at issue, 42 U.S.C. § 300jj-52, deals with information blocking. It gives ONC authority to create *exceptions* from what is considered information blocking in the context of EHI. That is, ONC is authorized to say only what does *not* constitute the blocking of EHI. In order to create those exceptions, ONC starts with a definition of EHI that is based on the definition of “health information” at 42 U.S. C. § 1320d(4)(B), which includes information that relates to past, present and future payment for the provision of health care to an individual. But from that rather uncontroversial proposal, ONC makes a statutorily unauthorized leap to say it may (at some unspecified point in time) *interpret* EHI to encompass general pricing information as well.

The mechanism that ONC eventually may use to require hospitals to disclose price information is unclear from the proposed rule’s preamble discussion. Because the proposed regulatory definition of EHI does not include price information, it may be that ONC intends to issue guidance describing its expectations and then seek to enforce that guidance against hospitals. (We note that, under the statute, notice and comment rulemaking must occur before a hospital can be penalized by an “appropriate disincentive” as the statute describes it.)

Both the structure and purpose behind the information blocking provision contradict ONC’s approach.

The information blocking provision in statute grants ONC “through rulemaking, [authority to] identify reasonable and necessary activities that do not constitute information blocking”² In other words, ONC’s rulemaking authority in the information blocking provision is limited to regulations creating *exceptions* to information blocking. ONC can use rulemaking to enumerate lists of practices that are *not* information blocking – but ONC *cannot* use the rulemaking authority to define conduct that *is* information blocking.³ Yet that is what ONC effectively seeks to do in stating price information must be disclosed.

Where an agency does not have an applicable basis of rulemaking authority, the agency lacks the power to adopt legally binding rules or regulations.⁴ Perhaps in recognition of this limitation, ONC says the regulatory definition of EHI “*may* include

² 42 U.S.C. § 300jj-52(a)(3) (emphasis added).

³ We note that there is no alternative basis of general (or specific) rulemaking authority that would authorize ONC to implement the contemplated proposal.

⁴ *City of Arlington v. FCC*, 133 S. Ct. 1863, 1884 (2013) (“[A] court cannot simply ask whether the statute is one that the agency administers; the question is whether authority over the particular ambiguity at issue has been delegated to the particular agency.”).

price information.”⁵ But, if that is the case, then ONC should include price information in the definition of EHI. The fact that it has not done so is telling.

We believe that the reason price information is not in the definition of EHI is because the information blocking provision simply does not confer authority on ONC to include it. Put another way, the information blocking provision does not give ONC authority to give an individual access to information that the individual would otherwise have no legal entitlement to view or receive. Rather, it prevents information technology developers and hospitals from *blocking or interfering with* an individual’s access to his or her health information. It is an unreasonable leap and a violation of the APA⁶ for ONC to say that “health information” includes information about payment that is or might be received by *completely unrelated third parties*.⁷

Moreover, if Congress intended to require providers to disclose price information, it would have spoken clearly. Congress would not hide such a mandate in vague language of an obscure provision of the statute, because “Congress ... does not alter [] fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.”⁸ To the contrary, Congress has spoken clearly when it intended to mandate disclosure of information – as it did in the Affordable Care Act when it required hospitals to make public a list of the standard charges for all items and services they provide,⁹ and in the Sunshine Act when it required disclosure and public reporting of confidential information about manufacturer payments to physicians.¹⁰ Given the highly confidential nature of price information, and highly controversial nature of requiring its public disclosure, Congress would not authorize ONC to include price information in the definition of EHI sub silentio.¹¹

Including Price Information in EHI Would be an Unreasonable Interpretation of the Statute. As discussed above, due to the structure of the information blocking provision, ONC has had to follow a tortured path in trying to require hospitals to disclose price information. We think that path is a legal dead end. The statute simply cannot support ONC’s strained and convoluted interpretation. It is ultra vires and exceeds ONC’s authority in violation of the APA.

⁵ 42 Fed. Reg. 7424, 7513 (Mar. 4, 2019) (emphasis added).

⁶ 5 U.S.C. § 706(C).

⁷ We note that ONC appears to be attempting to do something indirectly that it could not do directly: If ONC could require hospitals to provide their confidential price information to the government (which it cannot), that confidential commercial information would be protected from release under the Freedom of Information Act. 5 U.S.C. § 552(b)(4). ONC is attempting to avoid these constraints by threatening hospitals with penalties unless they disclose price information. But agencies may not do indirectly what they are not permitted to do directly. See *Cummings v. Missouri*, 71 U.S. 277, 278 (1867).

⁸ *Whitman v. American Trucking Ass’n*, 531 U.S. 457, 468 (2001).

⁹ Pub. L. No. 111-148 § 2718, 124 Stat. 119, 887.

¹⁰ See SSA § 1128G.

¹¹ See, e.g., *Director of Revenue of Mo. v. CoBank, ACB*, 531 U.S. 316, 323 (2001) (“[I]t would be surprising, indeed,” if Congress had effected a “radical” change in the law “sub silentio” via “technical and conforming amendments.”).

In addition, ONC's proposed interpretation of EHI to include price information would be arbitrary and capricious. ONC lists many unsubstantiated benefits that it asserts would result from disclosing price information while not mentioning any of the likely negative consequences. For example, ONC says that "price information could help increase competition that is based on the quality and value of the services patients receive."¹²

In fact, there is no reason to believe the proposal would enhance competition based on quality and value. Hospital-health plan price information is not a proxy for "quality."¹³ And disclosing price information actually would *inhibit* competition because it would create a platform for price fixing. Health plans would know what every other health plan was paying and could use that information indirectly to collude and drive prices below competitive levels, thereby *reducing* the incentives for actual competition in the marketplace, and threatening the viability of some of the nation's most vulnerable hospitals.

The FTC has been clear on this subject. In a letter to Minnesota state legislators, the Commission counseled against disclosure of health plan terms and urged that transparency be limited to "predicted out-of-pocket expenses, co-pays, and quality and performance comparisons of plans or provider."¹⁴ While the FTC focused on the providers' use of such information, a recent challenge to health plan consolidation pointed to the danger that collusion among commercial health plans would impede innovation and in drive prices below competitive levels for vulnerable providers without sharing any of savings derived from that illegal conduct for with consumers.¹⁵

Moreover, requiring hospitals to have a system that allows health plans to know how much *everyone else* is paying for a given procedure would be time and resource intensive. Such an unfunded mandate would increase burdens on already resource constrained hospitals and divert funds that otherwise could be used to enhance the quality of care.

ONC's failure to consider the risks of requiring the disclosure of price information and focus on unsubstantiated potential benefits, demonstrates that its decision to interpret EHI to include price information would be arbitrary and capricious in violation of the APA.¹⁶

¹² 42 Fed. Reg. 7424, 7513 (Mar. 4, 2019).

¹³ Previous transparency initiatives have not been found to improve quality. For example, the Sunshine Act required certain disclosures of manufacturer payments to doctors, but does not appear to have improved competition or quality.

¹⁴ Price Transparency or TMI?

¹⁵ "In highly concentrated [commercial health insurance] markets, already-large insurers are less constrained by competition and thus tend to find it more profitable to capture medical savings and increase premiums." *United States v. Anthem, Inc.*, 855 F.3d 345 (D.C. Cir. 2017) at 30.

¹⁶ 5 U.S.C. § 706(A).

Requiring Disclosure of Price Information May Violate the First Amendment. The AHA believes that ONC's interpretation of the information blocking provision may violate the First Amendment by compelling disclosure of confidential commercial information from contracts that hospitals enter into with health plans. As noted above, ONC failed to consider any of the negative consequences that might flow from requiring disclosure of price information. As a result, it is not clear that "the asserted governmental interest [in disclosing price information] is substantial."¹⁷ But, even assuming the proposal could be found to advance a substantial government interest, it is vastly overbroad: The government has a variety of tools at its disposal to improve choice, quality, and competition that do not require compelled speech by hospitals. Therefore, ONC should not be permitted to require disclosure of price information.

ADVANCING PRICE TRANSPARENCY

In addition to seeking comment on the inclusion of price information in the definition of EHI, ONC requests information on the many challenges to creating price transparency within health care. The first challenge is to adopt a common understanding of the type of information that will help patients make decisions about their care so that all stakeholders are working toward a common objective. We must then identify the types of services for which price estimates can reasonably be expected. Finally, we must address technical barriers to collecting the relevant information necessary for any one party – be it the provider, the health plan or a third party vendor – to generate an estimate.

Our members' long history working directly with patients to provide price estimates for care suggest that patients look for information on their out-of-pocket costs. Moreover, hospitals hear from patients that more data points are not always better. The addition of supplemental information – such as the chargemaster rates – can actually hinder patients' understanding of their costs by clouding over the important information and adding an unnecessary level of confusion. As noted previously, we especially do not support the broad disclosure of certain pricing data that could lead to anti-competitive behaviors that could hurt, not help, patients. According to the FTC, "when [price transparency] goes too far, it can actually harm competition and consumers."¹⁸ **We urge the agency to focus its efforts on patients' out-of-pocket costs to address the goal of price transparency and strongly oppose any policy that could implicate antitrust concerns.**

We also urge the agency to advance a common understanding of the types of services for which cost estimates may be feasible. The path to diagnosis and treatment can vary significantly based on the underlying health issue and the appropriate care pathway for a given individual. Additionally, estimates prior to emergencies could deter patients from receiving necessary emergency care. Research suggests that few health care services

¹⁷ See *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 566 (1980).

¹⁸ Price Transparency or TMI?

truly are “shoppable.” In fact, some researchers estimate that as little as 7 percent of health care services would meet the criteria.¹⁹ While providers and health plans working together can generally provide accurate price estimates for a small set of discrete services, the estimates vary widely for more complicated or variable sets of services. We support a collaborative public/private effort to identify the more common services for which patients should be able to expect price estimates so that the field can prioritize its efforts.

Finally, even developing price estimates for discrete services that are planned in advance can be challenging due to barriers in accessing all of the information necessary to generate an estimate. An estimate of a patient’s financial obligation requires specific information on the course of care, as well as the patient’s insurance information. While potential and returning patients often look to providers for the summation of this information, providers only know the particular services a patient is scheduled to receive (which, as previously noted, can change based on the inherent uncertainty during diagnosis and treatment); information on how the health plan will assess cost-sharing for a particular service depends on the health plan’s benefit design and the care ultimately received, which is why cost-sharing is often determined after a service is delivered.

Some mechanisms exist to make such information available to hospitals and health systems in advance; however, they frequently do not work. For example, our members report that the HIPAA standard eligibility transaction could, if returned from the health plan fully completed, provide much of this information. The health plans’ response often is limited though to “yes/no” about whether the individual is covered for the service. It does not include more detailed cost-sharing information, such as accurate information about where a patient is in their deductible. At that point, hospitals and health system staff must rely on a more manual process – calling the health plan for a one-on-one discussion about a patient’s coverage. This is not a scalable solution if the objective is to promote widespread access to timely, accurate and personalized cost-sharing information via the internet or mobile phone-based applications. **In order to promote a more seamless process for hospitals to provide patients adequate estimates of their financial obligations prior to care, ONC should work with CMS to enforce full compliance of the HIPAA standard eligibility transaction among health plans and providers to ensure universal adoption, including the exchange of information needed to provide personalized cost-sharing information to patients.** These standards ensure that sensitive data remains protected, while still allowing the vital exchange of information between necessary stakeholders.

We also encourage the continued development of Fast Healthcare Interoperability Resources (FHIR) financial resources, which will go further to allow for the integration of financial data into clinical decision making processes. To integrate price data into

¹⁹ Health Care Cost Institute, “Spending on Shoppable Services in Health Care,” March 2016. Accessed at: http://www.healthcostinstitute.org/files/Shoppable%20Services%20IB%203.2.16_0.pdf

electronic health record (EHR) systems, FHIR resources will need to be developed for the Accredited Standards Committee X12 transaction sets by including appropriate data categories in the US Core Data for Interoperability (USCDI). ONC will then need to work with Health Level Seven International to build out the appropriate FHIR financial resources for these transaction sets, which then can be used to make pricing information available to patients and providers at the point of ordering. Until the FHIR financial standards are fully defined, we cannot recommend universal adoption of these standards; however, we share the ultimate goal of integrating financial data into the clinical decision making process.

In addition to developing the technology necessary to scale price transparency solutions, we urge the agency to consider how to educate patients to interpret and use the data. Properly using price estimators requires a high level of health care literacy; and while providers and health plans have the resources available to help patients navigate and answer questions about the estimates and related information about their care, third-party apps often do not.

Another challenge, most relevant to the agency, is the issue of privacy and security of sensitive information when patients input insurance and condition information into third-party tools. At this point, the patient's data is no longer protected by HIPAA and can be sold, shared with third parties, or used to generate advertisements – often without the patient's knowledge or understanding. In addition, these third-party vendors are not required to encrypt the patient's data, opening the door to the potential for hacking and further exposing this sensitive data. While no longer liable for the patient's data at this point, hospitals are concerned about the potential harm this could cause our patients.

ADDRESSING SURPRISE BILLING THROUGH PRICE TRANSPARENCY

The AHA appreciates the administration's commitment to addressing surprise medical bills. We believe the last thing a patient should worry about while receiving health care services is an unanticipated medical bill that impacts their out-of-pocket costs and undermines the trust and confidence that patients have in their caregivers. Hospitals and health systems are deeply concerned about the impact of such bills and are committed to finding a solution that first and foremost protects patients. To that end, the AHA Board of Trustees earlier this year adopted a set of principles to help inform the development of a federal legislative solution.²⁰

ONC has asked whether including price information in the definition of EHI would be useful for a number of different policies being considered by HHS to minimize the incidences of surprise medical bills. The policies range from requiring hospitals to provide a single bill with all provider and facility charges as well as network status of all providers, requiring hospitals to provide patients with a binding quote for a "shoppable" hospital service, requiring hospitals to ensure that providers in their hospital only bill at

²⁰ <https://www.aha.org/initiativescampaigns/2019-02-20-surprise-billing-principles>

the “in-network” rate, and lastly, requiring hospitals to provide notice of their billing processes.

Incorporating price information into the definition of EHI will not solve or prevent surprise medical billing. Surprise bills are a direct result of a lack of a negotiated contract between the patient’s health plan and the hospital and/or physicians that provided their care. To address this issue, we support enhanced efforts to ensure that patients have access to adequate provider networks. When gaps in networks occur, such as in emergencies or when a patient reasonably could have expected for their providers to have been in-network, we support a change in federal law to protect them by disallowing balance billing. In addition, patients must be kept out of the middle of any dispute that may arise between the provider and the health plan regarding reimbursement.

Unlike a straightforward ban on balance billing, other proposed approaches to surprise billing are more complicated and put patients at risk of unintended consequences. Providing patients with a single bill is administratively and legally complicated and may create delays in billing for patients. Providing notice of network status, while not objectionable in theory, may not be feasible or actionable for patients in practice. Relying on notice requires that patients not only be able to understand their options but have the ability to make alternative arrangements. We do not believe patients should have to bear that burden during a vulnerable period as they seek treatment. Instead, they should simply not have to worry about receiving a balance bill. In addition, requiring hospitals to provide patients with a binding quote is inconsistent with the inherent uncertainty of health care. Hospitals strive to provide patients with all of the information they need to make important care decisions, including, to the extent practicable, estimated costs and information about billing processes. However, hospitals cannot control the unknowns about a patient’s condition, such as their reaction to a specific treatment, until care is underway. This makes providing binding quotes unfeasible for most health care services. Finally, legal considerations prevent hospitals and health systems from ensuring that non-contracting independent providers will bill only at the “in-network” rate.

We continue to urge the administration and Congress to protect patients by simply prohibiting balance billing. This straight forward solution protects patients while avoiding the complexity, burden and legal risks associated with other approaches.

STANDARD IMPLEMENTATION AND SPECIFICATIONS

Under the National Technology Transfer and Advancement Act, to carry out policy objectives, ONC is required to use technical standards developed or adopted by voluntary consensus standards bodies whenever practical. However, it has discretion to make exceptions, including the use of a government-unique standard. As such, ONC proposes to make four exceptions in this rule.

The AHA is very supportive of the development of technical standards and prefers they be developed or adopted by voluntary consensus standards bodies. These bodies, Standards Developing Organizations (SDOs), use a process that promotes the active participation and engagement of all affected stakeholders. They operate under the principles of openness; balance of interest; due process; an appeals process; and consensus.

The AHA acknowledges that in certain circumstances, there may be no voluntary consensus standards available to meet particular needs. In such cases, the use of market-driven standards developed in the private sector (consortia standards) may have merit. These consortia standards have been developed through a streamlined process that does not meet the full definition of voluntary consensus standards development. However, a faster/simpler process such as this may have an adverse impact in terms of assuring that these standards have been appropriately vetted, tested, validated or undergone an appropriate cost-benefit analysis. **As such, the pattern of bypassing SDOs is concerning to us.** For example, the proposed rule states that these consortia standards will include representation from those interested in the use cases supported by the standards and references health IT developers and health care providers. However, this is just a fraction of potential interested parties; there is no mention of vendors, health plans, clearinghouses or the general public to name but a few.

In addition, ONC has proposed to bypass SDO developed standards in certain cases, such as in the case of the Quality Reporting Data Architecture (QRDA) standard, because CMS has modified the standard for its own uses, making it difficult for hospitals to use their certified technology to submit quality measures to CMS electronically. We understand that ONC has proposed to use the CMS standard to make it easier for hospitals to submit their data to CMS. However, we are concerned that this opens the door for additional government agencies to specify their own standards or variations of SDO developed standards and obtain ONC recognition. ONC should carefully consider how it can encourage other federal agencies to utilize the SDO standards and engage with SDOs to modify the standards when they do not meet the agency's needs rather than creating their own unique standard or specification.

INFORMATION BLOCKING

TIMELINES

We are deeply concerned that ONC has proposed that the information blocking provisions would go into effect the day the rule is finalized – providing no time for hospitals and health systems to implement them. Yet, a number of exceptions would require not only modifications to current business models but also new accounting methods and significant documentation to ensure hospitals are complying with ONC's requirements. Since organizations will not know what is in the final rule until it is released, they will be left with no time to make these modifications or put systems into

place to ensure compliance with the regulations. This would leave hospitals and health systems at risk for penalties, even if they would technically qualify for an exception. **We strongly recommend that ONC provide an interim final rule with comment period rather than a final rule and that information blocking provisions be given an appropriate amount of time for implementation, at a minimum 18 months.**

DOCUMENTATION BURDEN

We understand from ONC's proposal that it intends to conduct, in conjunction with HHS's Office of Inspector General (OIG), investigations into information blocking complaints. As ONC described each of the exceptions, it is clear that in order to claim an exception when being investigated, a hospital would need to present significant documentation to demonstrate that it met "all applicable requirements and conditions of the exception at all relevant times." **We are concerned about the documentation burden this will impose on hospitals and health systems, particularly in light of the Administration's goal of reducing regulatory burden as described in ONC's Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs. Indeed, in 2016, we found that complying with health IT and the Meaningful Use program's regulatory requirements already cost the average sized hospital an astounding \$760,000 annually.²¹ This was in addition to \$411,000 in investments related to system upgrades during the year.**

When the Meaningful Use program was initially launched, CMS indicated that eligible hospitals and professionals (EHs and EPs respectively) could be subject to audits to ensure they met the measures but gave no direction on what documentation EHs/EPs would need to provide to auditors to demonstrate compliance. Consequently, in the first few years of the program, many organizations failed their audits not because they did not meet the measures but simply because they did not have adequate documentation. We are deeply concerned that hospitals and health systems would face similar risk under this proposed rule. Specifically, ONC has not made clear what type of documentation would be necessary to demonstrate that they met all requirements and conditions of an exception at all times. Additionally, we believe it would be impossible to document that requirements were met for some of the proposed exceptions. For example, how would a hospital document that its providers and staff did not counsel a patient not to provide consent (under the Protecting Privacy exception)? This seems impossible to document without recording individual conversations. **If ONC is going to put the burden of proof on regulated hospitals and health systems, it must provide numerous, detailed examples of acceptable documentation for each of the exceptions.** The penalties for information blocking are steep, and hospitals and health systems should not be put at risk of being labelled information blockers simply because ONC did not specify what documentation would be needed.

DATA COVERED BY INFORMATION BLOCKING PROVISIONS

²¹ Regulatory Overload. Assessing the Regulatory Burden on Health Systems, Hospitals and Post-Acute Providers. <https://www.aha.org/system/files/2018-02/regulatory-overload-report.pdf>

We appreciate and support the goal of making EHI more easily available to those who need it. EHI has been defined quite broadly, and our members often have reported that getting this extensive set of data out of EHRs can be difficult, particularly on an ongoing basis (as opposed to a one-time request). Yet, ONC has proposed that the information blocking provisions would apply to EHI without any caveats. This would mean that the set of data a hospital or health system would have to regularly make available would be quite broad and potentially very difficult to readily produce. **We urge ONC to consider the technology at hand and how easily it can export or exchange data. For example, limiting the information blocking provisions to the USCDI would allow for technology to advance and information sharing to advance with it.** Everyone would like to be able to share all data immediately, but it is simply not a reasonable expectation. Under the USCDI, ONC has laid out a plan for adding data elements, and we believe that it makes logical sense for the information blocking provisions to move at the same speed as the USCDI. This will ensure that, as we share data at greater levels, we are sharing accurate data that systems can interpret and use. Additionally, ONC can specify that when individuals are requesting access to their data that the information blocking provisions apply to the designated record set. This follows the HIPAA requirement for individual access requests, provides patients with a broad set of data, and already is technologically feasible for hospitals. **We specifically recommend that ONC limit information blocking to USCDI and the designated record set (for patient requests) either by clarifying the definition of information blocking or by ensuring that the exception for “Responding to Requests that Are Infeasible” expressly allows a hospital or health system to claim the exception for data elements that are not included in the USCDI or in the designated record set.**

EXCEPTIONS

Preventing Harm. We generally agree with ONC’s proposed exception for preventing harm. It is important to the physician-patient relationship that providers have the ability to withhold data they believe would be harmful to their patients. However, we do seek clarification from ONC on some of the specifics of the exception, per below.

Many hospitals and health systems have system-wide policies around withholding sensitive information, such as HIV test results, positive cancer results, etc. **We urge ONC to specify that such blanket policies are acceptable under this exception.**

In addition, state laws vary significantly on parental access to adolescent data. While some states allow parental access to all data, other states block all access or block access to certain types of data (e.g. sexual health). Because today’s technology cannot segment individual data elements, hospitals often set blanket policies that block parental access to data. Sometimes these policies block the adolescent patient from accessing their data over concerns that parents will gain access by forcing their child to provide them with their login credentials. **We urge ONC to specify that these types of blanket policies, which are intended to prevent harm to adolescent patients, would meet the exception requirements.**

Finally, ONC has proposed that hospitals and health systems could invoke this exception as a reason for not sharing substance use information that falls under 42 CFR Part 2 restrictions. However, it also specified that the rest of the record would need to be shared or the hospital or health system could be considered an information blocker. We are concerned about this proposal since the current technology does not allow for segmentation of data in a patient's chart at such a level. Specifically, health IT systems do not allow an individual data element, such as a lab result showing substance use or item in a problem list, to be segmented from other data. **Consequently, we urge ONC *not to require a record be shared if it contains sensitive health information until such time as health IT systems are able to appropriately segment data.*** Even then, we encourage ONC to understand the burden that will be placed on providers and their staff if they have to denote whether each data element in a patient's chart is sensitive. We also ask ONC to clarify that, under this exception, a treatment center governed by 42 CFR Part 2 would not be considered to be information blocking if they do not acknowledge that they have information on a patient for whom appropriate consent was not received or on file.

Promoting the Privacy of EHI. **We generally support the promoting privacy exception and appreciate ONC's statement that the information blocking provisions do not preempt HIPAA, state laws or 42 CFR Part 2 restrictions. However, we have several concerns about certain specific details of the proposal. First, we are concerned that, while ONC has stated that these laws are not preempted by the information blocking provisions, the agency has, in fact, preempted them by treating business associates the same as covered entities. Specifically, under the information blocking provisions, business associates would be required to share health information even if their business associate agreements (BAAs) expressly prohibit such sharing. As such, we urge ONC to clarify that under the promoting privacy exception, business associates *would be allowed to claim the exception when their BAAs prohibit them from sharing such data (which is a HIPAA requirement).***

In addition, ONC has proposed that to claim this exception that a precondition was not met (i.e. a hospital or health system has not obtained the consent or authorization of the patient and is required to do so prior to sharing), the actor must have done all things "reasonably necessary" to obtain the consent. ONC also specified that it may not have talked the individual out of providing her consent. While we understand that the goal is to ensure hospitals and health systems cannot use the lack of consent or authorization as a means to information block, we are concerned that the agency has not provided examples or information about what actions are sufficient to meet the "reasonably necessary" standard. Further, as mentioned above, we do not understand how a hospital or health system would demonstrate that one of its staff members did not talk an individual out of providing consent. Short of recording all conversations between staff and patients, we do not know how a hospital or health system could prove this negative.

Further, ONC seems to be putting the onus of collecting consent on the organization that holds the patient data, rather than on the organization who is requesting the data. This is not the current practice in the industry, and we disagree with ONC that this is where the responsibility should lie. Often, when data is requested about a patient, the patient is not present at the organization that holds the data, though they may very well be present at the organization that is requesting the data. Consequently, the proposal does not make logical sense. For example, if a hospital is located in a state that requires consent prior to data being shared for operations' purposes and a third party who is calculating quality measures for a payer requests data on 1,000 patients from a hospital, is it really the responsibility of the hospital to reach out to all 1,000 patients and collect their consent so the data can be shared? This is unreasonable. **Consequently, we urge ONC to modify this exception to make it clear that a hospital or health system may claim the exception when an entity requesting patient data does not communicate that it has obtained consent. This also is why we believe ONC should finalize its proposal to require certified health IT developers to implement the Consent2Share FHIR specification.** In fact, if ONC modifies this exception to put the onus on the appropriate party, many of our concerns about the lack of specificity on what it means to provide a meaningful opportunity or do what is reasonably necessary to collect consent would be removed since these would ultimately be removed from the exception. This would simplify this exception significantly.

In addition, ONC indicated that, under this exception, hospitals and health systems would have to demonstrate that requests by individuals that their EHI *not* be shared were initiated by the individual and that they were not convinced to make such a request by the organization. We reiterate that it is unclear how a hospital or health system would demonstrate that such a request was initiated by the individual and that the organization did not influence the individual's request. Since the proof of burden is on the hospital and health system, ONC must provide specificity on what type of documentation or proof would suffice to demonstrate that the organization met the exception, or simply eliminate this requirement under the exception.

Finally, we appreciate ONC's consideration of hospitals and health systems that operate in multiple states, and the agency's request for feedback on including an accommodation that would allow them to set a single policy for all of their sites that follows the state laws of one of the states in which it operates. **We strongly support this accommodation and urge ONC to finalize it.** Many of our members operate in multiple states, some of which require specific consents and authorizations prior to sharing a patient's health information. It is difficult for these hospitals and health systems to set varying policies across their sites, particularly when they are utilizing the same EHR system.

Promoting the Security of EHI. We appreciate that ONC proposed an exception for maintaining security practices that might prevent the exchange of EHI but protect patient data. However, we are concerned that the overall tone of the proposal seems to force a reactive security posture rather than a proactive security posture. Specifically,

while ONC makes clear that security policies could be linked to actual risks via a HIPAA risk assessment or could be linked to the HIPAA Security Rule, the agency also states that such linkage may not be dispositive of information blocking. ONC also discusses that security policies must be related to a particular threat – in the examples provided, such policies are linked to an organization responding to a security instance and issuing a policy rather than setting a proactive policy to prevent incidents.

We understand that ONC is attempting to ensure that arbitrary policies are not used to information block. However, we are concerned that its proposal that all policies must be linked to a national consensus-based standard or best practice, and its statement that the HIPAA Security Rule may not be enough of a link, could force hospitals and health systems to lower their security standards. This could, in turn, threaten the security of patient data. ONC is not considering the HIPAA requirements hospitals and health systems face, particularly the penalties that may be imposed if a breach occurs. **Under ONC's proposal, it is asking hospitals to choose between HIPAA penalties and information blocking penalties, putting them in a no-win situation. We urge ONC to consider a better method for testing security policies other than requiring that they align to consensus-based standards/best practices or that they only be in response to a threat or security issue that has already occurred. Instead, it should ensure that hospitals and health systems can set proactive security policies that will not force them to choose between protecting patient data or being labelled information blockers.**

Recovering Costs of Reasonably Incurred. In the rule's preamble, ONC indicated that non-observational health information is still considered EHI and includes data "created through aggregation, algorithms, and other techniques that transform observational health information into fundamentally new data or insights that are not obvious from the observational information alone. This could include, for example, population-level trends, predictive analytics, risk scores, and EHI used for comparisons and benchmarking activities." While ONC specifies that an information blocking investigation would be less likely to be triggered by not sharing this type of data, it also states that such data is regulated by the information blocking provisions. This, in turn, means that other than recovering costs reasonably incurred, hospitals and health systems would not be able to charge fees for access to such data, despite the fact that they have invested in the technology and software to create it. **This is concerning to us – transforming health information into something new, such as clinical decision support, quality measures, risk scores, etc. takes significant effort and technology and is fundamentally different than simply recording data about a patient (such as vitals, problems, medications, etc.).**

Despite ONC's assertion that this exception allows for the generation of a profit, it, in fact, does not when the regulatory text is interpreted in the most literal fashion. Our understanding is that ONC wishes to bring more competition into the health IT space by ensuring that information is not blocked from organizations and companies that wish to transform it into something new. However, in its efforts to ensure that EHR vendors do

not perpetuate rent-seeking behaviors, ONC has inadvertently disadvantaged entities who transform data, by ensuring they cannot generate a profit from such work. The result of ONC's proposal would be multi-faceted:

- New technology companies would not enter the market;
- Vendors who provide key services, such as population health and analytics services would be put out of business, leaving hospitals and health systems with only their EHR vendor to support all of their technology needs;
- Health systems who transform data by creating risk scoring algorithms, clinical decision support, safety analysis, etc. would no longer create these needed services; and
- Innovation could be hampered by including hard and fast rules and definitions in regulation – technology is advancing rapidly and it is unclear what data uses will be possible in the future.

As such, we urge ONC to exclude non-observational data from being considered EHI. This would remove such data from being regulated by the information blocking provisions and encourage an open, competitive, free market for data services. If ONC fails to do so, it would lead to a significant market failure that will ultimately harm patients.

Responding to Requests that Are Infeasible. We appreciate that ONC included an exception for requests that are infeasible. While we generally agree with the exception, we ask that ONC clarify its statements on providing alternative means for accessing information. Our understanding is that, under the proposal, a hospital or health system who is a member of a network could offer providing the data via the network as an alternative means to creating a one-off interface with an organization, provided the information being sought is available via the network. However, ONC also states that they would balance such an offer with the cost and burden for the requestor on using the alternative means to access information. We urge ONC to clarify how they would balance these two conflicting provisions. For example, if a hospital or health system has spent considerable time and money to join and maintain a connection to a network, how would ONC balance that against the cost of joining to the other party? Would it calculate whether such a network connection would only provide access to one entity versus many? We also request that ONC include in this exception a clear safe lane for all actors related to the Trusted Exchange Framework and Common Agreement (TEFCA). Specifically, ONC should add a provision to the exception that would enable entities who have joined the TEFCA to claim this exception if a requestor or third party refused to join the TEFCA in order to gain access and instead demanded a one-off interface. We believe it is important to provide a clear, safe lane under this exception.

TEFCA Exception Request for Information. ONC requested comment on whether to include an exception for policies, contract terms and practices that are necessary for participation in the TEFCA. Based on this request, we understand that this exception would allow organizations who participate in the TEFCA to claim it as an exception for a particular practice if investigated for information blocking. We ask ONC to clarify that if a

hospital does not share EHI because the TEFCA does not require or include such sharing in the Common Agreement, that they could claim this exception. If a third party app used by an individual has not followed the security protocols of the TEFCA by, for example, not identity proofing individuals, then a hospital should be able to refuse to share information with such an app and claim the TEFCA exception, provided the hospital is a participant in TEFCA. The TEFCA has the potential to provide hospitals and health systems with an easy way to exchange health information – it is low cost and does not require multiple interfaces or APIs. **Therefore, we strongly support such an exception, which would encourage actors to participate in the TEFCA and would provide an important “safe lane” for hospitals and health systems, particularly when coupled with the exception for “Responding to Requests that Are Infeasible.”**

New Exception: Protecting Privileged Information. We are concerned that because the definitions ONC has proposed are very broad, particularly the definition for EHI, data that organizations create from observational health information about quality and safety would be required to be exchanged freely with other organizations. This could lead to hospitals and health systems shutting down quality programs or failing to report data to patient safety organizations (PSOs) for fear such data would be made publicly available or used against them during litigation. There also could be situations where law firms mine this data from hospitals specifically to create lawsuits. **Therefore, we strongly urge ONC to create a new exception that enables actors to claim the exception if they are protecting privileged information.** This would provide an appropriate protection that would allow hospitals and health systems to continue their quality programs and report data as needed to PSOs without having to be concerned that they will face legal repercussions. ONC could work with the field to identify which data would be considered privileged and subject to this exception. We understand that the exception likely would require entities to have a policy in place regarding such data.

DISINCENTIVES FOR HEALTH CARE PROVIDERS – REQUEST FOR INFORMATION

HHS requests information on “more effective deterrents” to information blocking. It notes that the law requires that HHS, to the extent possible, not duplicate penalties that would otherwise apply for information blocking as of the day of enactment of the 21st Century Cures Act. However, as the agency is well aware, eligible hospitals and physicians participating in the Medicare Promoting Interoperability Program must already attest that they do not “information block” in order to avoid failing the program. There are financial penalties attached to failure and they are steep – for hospitals, a 75 percent reduction in their inpatient prospective payment system market basket. **As such, providers clearly already have substantial disincentives to information blocking, and we oppose enactment of additional penalties, which are unnecessary and also would violate HHS’s requirement that it avoid duplicating existing penalty structures.**

CONDITIONS AND MAINTENANCE OF CERTIFICATION

When patients have access to their health information they can engage more fully in their care and experience better outcomes; as such, we strongly support patients having easy access to their health information so that they can be partners in their care. **However, we do not believe that patients should have to sacrifice data protections and data privacy in order to receive easy access to their health information.** We are deeply concerned that third party applications and tools that are not governed by HIPAA are increasingly accessing patient data and using it in ways patients are likely unaware of. While we applaud CMS for putting limitations on how data from its own APIs can be used (they prohibit apps from selling the data), at least half of the developers who are currently connected to CMS' API use patient data for advertising to patients (ultimately selling access without selling patient data). Further, because of the fee limitations that ONC has proposed, these third parties are accessing patient data for free and then turning around and monetizing it. Some even charge the patient for using the app, though they are accessing data for free. Patients data is their own, and no organization, whether regulated by HIPAA or not, should be allowed to capitalize and monetize their data without the patient fully understanding what is occurring and agreeing to it. **We urge ONC to consider the ramifications of its proposals and consider ways that we can help patients get easy access to their data without sacrificing their control or the protections HIPAA offers.**

COST SHIFTING TO HOSPITALS

ONC proposes that API Technology Suppliers may only charge API Data Suppliers for use of the certified APIs. We understand that the goal of such a policy would be to ensure that API Technology Suppliers are not "double dipping" with their fees and charging both API Users and API Data Suppliers. However, we are concerned that an unintentional consequence of ONC's proposal (particularly when coupled with the information blocking exceptions that make sharing data the default setting) is that API Data Suppliers would bear the full cost of data exchange, even when such exchange does not benefit their organization or their patients. As such, we urge ONC to modify its policy to ensure that API Data Suppliers, which would include hospitals, health systems, and ambulatory providers, are not facing significantly increased costs because API Users cannot be charged. We also ask that ONC clarify if API Data Suppliers would be allowed to recoup costs from API Users in light of the information blocking provisions.

REMOVAL OF GAG CLAUSES

ONC proposes that, as a condition of certification, health IT developers would not be able to contractually restrict their users from communicating about the usability, interoperability, security, user experience or business practices of the developer. **We strongly support this proposal, which would effectively eliminate gag clauses in contracts and urge ONC to finalize it.** These gag clauses have been used to prevent

hospitals from working with preferred partners, publishing journal articles that contain important screen shots, reporting safety-related issues, and working collaboratively across the field to solve interoperability issues. In fact, we encourage ONC to shorten the six-month timeline that it has proposed for health IT developers to notify their customers that such clauses are no longer in effect. There is no reason why a developer would need six months to conduct such notification and removing these gag clauses as quickly as possible is in the best interest of, among others, patients and hospitals. We believe that allowing three months for the initial notification would be sufficient.

API DATA PROVIDERS - SOLE AUTHORITY

ONC proposes that API Data Providers (which we interpret as hospitals, health systems, providers, etc.) would have sole authority and autonomy to provide access to APIs they have deployed. This proposal would ensure that EHR vendors could not withhold access from a third party that a hospital or health system wants to work with. Indeed, our members often have reported instances where they want to work with a third party to provide population health or care coordination tools but are prevented from doing so because their EHR vendor withholds access to the health information in the EHR. **As such, we strongly support preventing API Technology Suppliers (which we interpret as certified health IT developers) from withholding access when a hospital or health system wants to work with another vendor.**

PARTICIPATION IN TEFCA

As proposed, the TEFCA will be important for the field insofar as it provides an easy means to exchange health information. It also will be important for certified health IT developers to join Qualified Health Information Networks (QHINs) to provide the “single on-ramp” proposed in the TEFCA. This will be the easiest method for hospitals and health systems to participate. **Since in CMS’s proposed interoperability rule, it would require hospitals and health systems to participate in a trusted exchange network, we believe it also is important for ONC to require certified health IT developers to participate in TEFCA as a condition of certification.** We are concerned that if ONC does not make this a condition of participation and CMS finalizes its proposal, vendors may not join a QHIN, leaving hospitals and health systems with no way to join or a significant cost to join and unable to meet CMS’s requirements.

NEW CERTIFICATION CRITERIA

ELECTRONIC HEALTH INFORMATION DATA EXPORT

Hospitals and health systems often face “vendor lock-in.” Specifically, they have spent years inputting patient health information into their EHR systems or other third party products, and the inability to get such data out of the system prevents them from

changing systems. In fact, our members have reported that health IT developers often purposefully make it difficult for their customers to get their data out of the system to ensure they will not switch to a competitor's product. While we appreciate ONC's current requirement in the 2015 Edition that developers must be able to export all patient records in a consolidated clinical document architecture (C-CDA) format, this has proven to be insufficient for switching systems. The C-CDA contains only a limited set of data – not nearly all of the data in a patient record. **As such, we strongly support ONC's proposed criterion that would require certified health IT developers to be able to export all data from all patient records that the developer produces or maintains. We also support the requirement that such export be accompanied by a data map.** Without such a map it would not be possible for another vendor to interpret the export and input data into the correct place in the new system.

We also are supportive of providing a full data export of EHI for patients upon request – it is important for patients to have free, easy access to their health information. We support ONC's proposal that such an export would be generated by a user of the system. In addition, we understand that ONC may be considering broadening the criteria to enable a third party health IT developer or app to request such data on behalf of the patient, potentially via an API. While EHR systems can certainly provide such a capability from a technical perspective, we are concerned that ONC may not be adequately considering the bandwidth necessary to provide such an export. If an individual has been a patient of a hospital or health system for many years, the breadth of their EHI likely will be quite large. While performing such an export for one patient may seem trivial, we can envision a scenario where a third party begins pulling such an export on a daily basis for a large patient population. Of note, many of the third party patient apps are currently performing a daily auto-query for the Common Clinical Data Set. While the bandwidth for this is manageable (though not ideal) if these developers follow the same process for the full EHI export, it could lead to system crashes, creating a significant patient safety risk for hospitals. **We encourage ONC to consider these bandwidth issues and take into account the range of software architectures used in the market, from client side to software as a service (SaaS).** While patient access to data is vitally important, it must not put at risk patients who are actively being cared for in a hospital or health system.

CONSENT MANAGEMENT FOR APIs

Under HIPAA, 42 CFR Part 2, and numerous state laws, hospitals and health systems are required to obtain consent from patients prior to sharing their health information. ONC has made it clear in the information blocking provisions that they must have policies in place for obtaining and recording consent, and that they cannot refuse to release EHI when consent has been properly obtained. However, the organization holding data is not always the organization obtaining consent from patients, and there is currently no standard being used to electronically communicate to an organization that appropriate consent has been obtained when asking for data. As such, ONC has proposed that health IT developers who are certified for the FHIR APIs also would need

to be certified for the Consent2Share FHIR specifications. **We urge ONC to finalize its proposal to require certification to the Consent2Share FHIR specification.** Without this technical standard, it will be incredibly difficult, if not impossible, for the field to know whether appropriate consent has been obtained prior to releasing health information. Further, we are concerned that without such capabilities, hospitals and health systems could be accused of information blocking because they cannot verify that a patient has given consent for their EHI to be shared. If ONC does not finalize this technical requirement, we believe the agency should provide an appropriate exception in the information blocking provisions that will ensure hospitals and health systems cannot be accused of information blocking because they do not know if another organization has obtained consent from patients.

LICENSING OF INTEROPERABILITY ELEMENTS ON REASONABLE AND NON-DISCRIMINATORY TERMS

The AHA appreciates and supports the proposed rule's goal of promoting interoperability of health information technology. We also support the goal of ensuring that interoperability is affordable in the health care sector through licensing programs for technology related to vital business processes such as billing, quality assurance and claims administration. Health information networks and other entities, including non-profit organizations, play an important role in the health information technology ecosystem by developing and maintaining health information technology interoperability elements, such as code sets, software and APIs, and making them available to hospitals and other healthcare organizations through licensing arrangements.

We support the licensing of interoperability elements on “reasonable and non-discriminatory” (RAND) terms with the flexibility to assure that licensing models can meet the needs of direct and ultimate users. Rural hospitals, for example, are often ultimate users of code sets, software and APIs. It is important that licensing terms can be adjusted to respond to those and other hospitals that are in financial distress or facing unique circumstances to assure that their ability to make use of codes, APIs or other health information technology critical to their viability is not compromised. **To that end, we support an affirmation that flexibility with respect to the RAND terms is consistent with the “careful consideration of relevant facts and circumstances in individual cases” on which the interoperability framework rests.**

The proposed rule provides that RAND terms cannot be based on:

- Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; or
- The revenue or other value the requestor may derive from access, exchange or use of electronic health information obtained via the interoperability elements, including the secondary use of such electronic health information.

“Interoperability element” is defined to include certain hardware, software, technical information and technology or services relating to the access, exchange, or use of EHI for any purpose.

There are a number of licensing arrangements that should be consistent with the RAND terms and also able to respond with flexibility to users’ particular circumstances. Take, for instance, a licensing arrangement that takes account of an ultimate user base made up of hospitals of different sizes. A licensing fee that is tiered so that there is a more modest fee for small, critical access, rural or frontier hospital users than others, for example, would undeniably promote interoperability for that group of hospitals.

It is the AHA’s view that flexibility in licensing arrangements is entirely consistent with the intent of the proposed rule because such arrangements are not “inherently likely to interfere with access, exchange, or use of EHI.” HHS has acknowledged that “different fee structures or other terms may reflect genuine differences in the cost, quality or value of the EHI and the effort required to provide access, exchange or use.”

Licensing arrangements where the royalty fee is not based on the user’s: (1) sales of the technology, (2) profits derived from the use of the technology, or (3) other value derived from the use of the technology, including the secondary use of EHI associated with use of the technology, should fit comfortably within RAND terms that incorporate options for flexibility. RAND terms should be interpreted with enough flexibility to permit use of a metric that differentiates between users based upon their size and level of business activity, but is not directly derived from revenues. For example, in some cases, daily claim volume may be the most accurate and meaningful measure for classifying the size of a customer organization, rather than the number of end-users, hospital beds or affiliated physicians. The AHA continues to support licensing health information in a reasonable and non-discriminatory manner with the flexibility to meet the needs of hospital and hospital system users.